

Wer Zugang zum Quellcode hat, trägt ein besonderes Risiko

27.08.2026, 09:46 | Handel, Wirtschaft, Finanzen, Banken & Versicherungen

Pressemitteilung von: *Validato*



Wer Zugang zum Quellcode hat, trägt ein besonderes Risiko

Warum IT-Unternehmen sensible Rollen zunehmend differenziert prüfen und was dabei datenschutzrechtlich entscheidend ist.

Quellcode, Konstruktionsdaten und Produktions-Know-how gehören zu den wertvollsten Vermögenswerten produzierender und softwarenaher Unternehmen. Validato, Anbieter für Background-Checks und Human Risk Management mit Sitz in Zürich, weist darauf hin, dass Personen mit Zugriff auf diese Informationen ein besonderes Risiko tragen – und dass eine differenzierte, datenschutzkonforme Prüfung dieser Rollen zunehmend Teil moderner Sicherheitskonzepte wird.

Quellcode als Kronjuwelen

Für softwarenahe Unternehmen ist der Quellcode oft der zentrale Wettbewerbsvorteil. Nach Einschätzung von Validato rechtfertigt dieser Wert eine gezielt vertiefte Prüfung von Rollen mit entsprechendem Zugriff – losgelöst vom allgemeinen Prüfumfang anderer Positionen. Ein Abfluss von Quellcode kann Wettbewerbern nicht nur Entwicklungszeit, sondern auch Einblick in strategische Produktentscheidungen verschaffen. Nach Einschätzung von Validato wiegt dieser Schaden oft schwerer als der unmittelbare finanzielle Verlust durch einen einzelnen Sicherheitsvorfall.

Nicht jeder Entwickler ist gleich exponiert

Zugriffsrechte auf Repositories, Produktionssysteme oder Deployment-Pipelines unterscheiden sich innerhalb eines Entwicklerteams teils erheblich. Validato empfiehlt, die Prüftiefe an den tatsächlichen Zugriffsumfang einer Rolle zu koppeln, nicht an den Jobtitel. Ein Praktikant mit eingeschränktem Lesezugriff auf einen einzelnen Programmteil stellt ein anderes Risiko dar als eine Senior-Entwicklerin mit Schreibrechten auf die gesamte Codebasis. Validato empfiehlt, diese Unterschiede bei der Modulauswahl explizit zu berücksichtigen, statt alle Entwicklerrollen gleich zu behandeln.

Differenzierte statt pauschale Prüfung

Aus den verfügbaren Screening-Modulen wählen Unternehmen laut Validato erfahrungsgemäss typischerweise vier bis

fünf pro Position aus – abhängig vom konkreten Risiko, das mit der jeweiligen Rolle verbunden ist. Zu den häufig gewählten Modulen zählen dabei Identitätsverifizierung, Ausbildungsnachweise und Sanktionslistenabgleich. Weitergehende Module wie ein Strafregistrauszug kommen laut Validato gezielt bei Rollen mit besonders sensiblem Zugriff hinzu.

Was datenschutzrechtlich entscheidend ist

Nach DSGVO und BDSG muss jede zusätzliche Prüftiefe für eine bestimmte Rolle erforderlich und verhältnismässig sein. Ein pauschal begründeter „Vollcheck“ für alle Entwicklerinnen und Entwickler lässt sich laut Validato datenschutzrechtlich kaum rechtfertigen. Unternehmen müssen im Zweifel darlegen können, warum eine bestimmte Prüfung für eine konkrete Rolle notwendig war und nicht lediglich wünschenswert. Nach Einschätzung von Validato lässt sich dieser Nachweis nur führen, wenn die Zuordnung von Rolle und Prüfmodul von Anfang an dokumentiert wird.

Dokumentation als Absicherung

Validato empfiehlt, die Zuordnung von Rolle zu Prüfmodul schriftlich zu dokumentieren – inklusive Begründung, warum ein bestimmtes Modul für eine bestimmte Position angemessen ist, um im Streitfall die Erforderlichkeit nachweisen zu können. Eine solche Dokumentation muss laut Validato nicht aufwändig sein, sollte aber nachvollziehbar festhalten, welches Risiko mit einer Position verbunden ist und welches Modul dieses Risiko adressiert. Im Idealfall lässt sich diese Zuordnung für ganze Rollenkategorien einmalig festlegen und wiederverwenden.

Validato: Modulare Prüfung sensibler Rollen

Validato bietet dafür 18 einzeln wählbare Screening-Module auf einer ISO-27001-zertifizierten Plattform. Ergebnisse liegen für die meisten Module innerhalb weniger Minuten vor, buchbar über WebApp oder API ohne Setup- oder Jahresgebühren – ein Modell, das sich nach Angaben von Validato besonders für Unternehmen eignet, die mehrere sensible Rollen parallel prüfen müssen. „Wer Zugang zum Quellcode hat, verdient eine sorgfältigere Prüfung – aber keine, die über das Notwendige hinausgeht“, so Reto Marti - Managing Partner von Validato. Genau diese Balance versucht Validato in jedem Modul abzubilden. Unternehmen können auf diese Weise für unterschiedliche Entwicklerrollen unterschiedliche Modulkombinationen hinterlegen, ohne den Prüfprozess für jede Neueinstellung manuell neu zusammenzustellen. Das reduziert laut Validato sowohl den administrativen Aufwand als auch das Risiko einer inkonsistenten Prüfpraxis.

Validato AG

Claridenstraße 34
8002 Zürich
Schweiz

RetoMarti (Managing Partner)

+41 44 515 77 77

reto.marti@validato.com

validato.com/de-de

Portrait

Die Validato AG mit Sitz in Zürich entwickelt und betreibt eine konfigurierbare Background-Screening- und Human-

Risk-Management-Plattform mit Fokus auf den DACH-Markt. Über 18 Module deckt Validato den gesamten Lifecycle ab — von Pre-Employment-Screening über In-Employment- und Re-Screening bis hin zu Third-Party-Screening, Lieferantenprüfung und Due Diligence. Die Plattform arbeitet mit einem Pay-per-Use-Modell, ist vollständig DSGVO- und nDSG-konform und auf die Rahmenwerke NIS2, DORA, KRITIS-Dachgesetz, DIN SPEC 14027:2026-04, BSI C5:2026, AI Act, LkSG sowie ISO 27001 ausgerichtet.

News-ID: 1321222 • Views: 92 (Stand: 13.09.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/1321222/Wer-Zugang-zum-Quellcode-hat-traegt-ein-besonderes-Risiko.html>